【注意喚起文書】

「ドッペルゲンガー・ドメインへの漏えい事案」を踏まえた

電子メールによる個人データの取扱いについての注意喚起

令和４年 12 月 28 日
個人情報保護委員会事務局

個人情報取扱事業者におかれては、個人データを持ち出す際のルールを決めるなどの安全管理措置を講じられていることと思いますが、以下のとおり電子メールを転送した際の漏えい事案が発生しましたので、ご注意ください。

なお、ドッペルゲンガー・ドメインについては※を参照ください。

【事案の概要と注意すべき点】

事業者が従業者に付与している電子メールアドレスで受信したメールにつき、従業者が個人的に取得・管理している電子メールアドレスへ自動転送されるよう設定を行っていたところ、当該設定時に転送先の電子メールアドレスに誤りがあったため、個人データを含む電子メールが当該誤った電子メールアドレスに送信され、個人データの漏えいが発生した。

個人データを外部に持ち出すにあたり、ＵＳＢメモリ等の電子媒体で持ち出す場合については、持ち出しが認められている個人データであるかを確認する、紛失や盗難対策（パスワード設定、暗号化等）が施された電子媒体を使用する等、規程その他の組織として定められている安全管理措置に関するルールに沿った取扱いが徹底できていても、電子メールで受領した個人データを外部に転送する場合については、従業者は持ち出しているという認識を持ちにくく、ルールの対象であることを認識しないまま、ルールを遵守せずに行ってしまいがちです。このような状況を踏まえ、あらためて規程その他の安全管理措置や従業者の監督が必要です。

【個人データを含む電子メールを外部に転送する場合の注意すべきポイント】

○ 従業者個人のメールアドレス宛てに電子メールの転送を許容する場合、個人情報取扱事業者において従業者個人の電子メールアドレスやパソコン等のセキュリティ対策の実施状況を把握することが困難であるため、安全管理上注意が必要。

○ 電子メールの転送を自動設定で行う場合は、個人データの持ち出しにおける制限等のルールを設けていても、受け取った電子メールの内容を確認することなく転送することとなるため、特に危険性が高い。やむを得ず実施する場合は、宛先等に注意が必要であり、対策として、必要に応じ転送先のメールアドレスの申請を義務づける等の

方法が考えられる。

また、通常、存在しないアドレス宛に電子メールを送信した場合には、エラーメッセージが返送され、誤送信に気が付くことができるが、自動転送設定時に、例えば、〇〇mail.com を〇〇mai.com と一文字入力が漏れるなど誤った場合（特にフリーメールアドレスは要注意）には、一般的に「ドッペルゲンガー・ドメイン」と呼ばれるアドレス宛に送信され、悪意の第三者に受信されるケースもあるため、注意が必要。

事業者の皆様におかれては上記を踏まえ、電子メールに付随した個人データを含む、個人データを持ち出す際のルールを今一度ご確認いただき、必要に合わせて適切な規程の整備その他の安全管理措置等を講じていただくことが重要です。

※「ドッペルゲンガー・ドメイン」とは、フリーメールアドレスなどの正規のドメインにおけるタイプミス（例：〇〇mail.com を〇〇mai.com と一文字入力が漏れる）や誤認識しやすいドメインを取得し、ユーザーが誤ってアクセスしたり、電子メールを誤送信したりすることで情報収集することを目的としたものです。

「ドッペルゲンガー・ドメイン」宛ての電子メールの誤送信防止のためには、規程において電子メールの送付先を制限する等の組織的安全管理措置、サーバー側において、あらかじめ誤りやすい電子メールアドレス宛ての電子メールを送信できないよう設定する、電子メールを扱うためのソフトウェアにおいて、送信前に注意喚起されるように設定するなどの技術的安全管理措置を講ずるなどの方法があります。